REMARKS

The Office Action objected to Claims 1-10 due to informalities. Applicant has amended Claims 1-10 according to incorporate amendments suggested by the Examiner.

The present invention is directed towards estimating the cipher strength of a Feistel encryption algorithm while decrypting the algorithm. (Pg. 1). It accomplishes this by calculating a parameter A, which is a parameter that allows an extended key to be calculated by a simple logic operation with a known value like the equivalent key. XOR-ing the extended key with a constant produces the equivalent key. The extended key can thus be calculated easily from the equivalent key based on the known constant.

Thus, as seen in Figure 1, the estimated plaintext calculating part 11 accepts a predetermined-step stirred text and outputs an estimated plaintext to the encryption control part 2. The present invention estimates a plaintext based on the parameter A and the stirred text and then encrypts the plaintext. It also outputs an estimated predetermined-step stirred text to the key verification part 4. The key verification part 4 also receives an estimated ciphertext from the encryption control part 2. Ciphertext is estimated by accepting stirred text, then estimating a parameter A by exhaustive search at the first step.

The key verification part 4 then uses both the predetermined-step stirred text and estimated ciphertext to calculate a last-step estimated extended key if possible. If however, the calculation is impossible, it sends a calculation impossible signal to decryption control part 5. The decryption control part 5 can then send a recalculate signal to the estimated plaintext calculating part 11 to recalculate parameter A. For example, a cryptanalysis condition relating to a higher order difference held between the stirred text and stirred text at a second predetermined

step estimated based on the ciphertext is utilized. It can be utilized to calculate a right extended key at the last step based on stirred text at the first step and unstirred text at a given step.

Thus, the process is repeated until a last-step estimated extended key is calculated.

The Office Action rejected Claims 1-10 under 35 U.S.C. § 103(a) as being unpatentable over *Coppersmith et al.* (U.S. 6,189,095) in view of *Ohkuma et al.* (U.S. 7,227,948).

Coppersmith does not teach or suggest "A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus." The Office Action cites to Column 5, lines 41-67 in *Coppersmith* for the above feature of the present invention. However, *Coppersmith* only discloses providing a user with a choice of choosing the strength of a cipher. Thus, in *Coppersmith*, the term "evaluation" is used in the context of a user evaluating which cipher strength the user whishes to use. The user does not evaluate how strong the cipher is since the cipher strength is already known.

Coppersmith also does not disclose "an estimated plaintext calculating part for accepting predetermined-step stirred text being stirred text at a predetermined step, calculating an estimated parameter A, estimated as a parameter A, determined from a predetermined-step extended key being an extended key at a predetermined step, and calculating estimated plaintext based on the predetermined-step stirred text and the estimated parameter A." *Coppersmith* only discloses determining which hardware and software to use to run the cipher based on variable information used by the algorithm such as key length, block length, number of rounds of expansion, number of stages, etc. to optimize performance. *Coppersmith* does not teach using an estimated parameter A, which is, for example, an equivalent key at a predetermined step. The

hardware and software used *Coppersmith* is not an extended key and although the hardware and software run the algorithm, the logical or mathematical characteristics of the hardware and software are not used to actually calculate an estimated plaintext.

In contrast, in the present invention, the estimated parameter A, a parameter that allows an extended key to be calculated by a simple logic operation with a known value like the equivalent key. This allows for the calculation of the extended key if the parameter A and the equivalent key are known. (Pg. 11 – 12).

Coppersmith also does not teach or suggest "an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part." *Coppersmith* does not disclose the use of an encryption control part that calculates an estimated ciphertext based on the estimated plaintext from the estimated plaintext calculating part. *Coppersmith* only discloses an expansion function that uses a bitwise rotation in a plurality of rounds for encryption. There is no indication that it uses an estimated plaintext to calculate the estimated ciphertext. Furthermore, there is no indication that the estimated plaintext is received from the estimated plaintext calculating part or more specifically an estimated plaintext calculating part having the features of the present invention.

Coppersmith also fails to recite "a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step stirred text accepted by the estimated plaintext calculating part and the estimated ciphertext calculated under the control of the encryption control part." *Coppersmith* discloses an expanded key array which is populated through the use of an input key. The expanded key array is created through concatenation of the input key with a counter i for n iterations. Therefore, *Coppersmith* turns a

single key into a plurality of keys by combining a counter i that changes with each iteration with the input key. Thus, there is no indication that *Coppersmith* creates encryption keys using higher order difference, uses higher order differences, or uses higher order differences based on the any sort of stirred text and estimated ciphertext.

Coppersmith also fails to teach or suggest "processing it by an algebraic technique to try to calculate a last-step estimated extended key estimated as an extended key at a last step." Again, *Coppersmith* merely teaches using an input key to create an expanded key array. It uses an iteration of n times to create n different keys. Each key in the expanded key array is not created through an algebraic technique as can be seen by the function PRF where PRF is some pseudorandom function using the concatenation of input parameters I and K. Thus, *Coppersmith* populates an expanded key through concatenation but not through any algebraic technique. Furthermore, there is no indication that expanded key array E[n-1], the last value in the expanded key array, is an extended key at the last step. In *Coppersmith*, the population of the expanded key array is not the decryption of an encryption algorithm, such as a Feistel encryption algorithm, but rather key expansion.

In contrast, in the present invention, the key verification part 4 uses an algebraic technique to try to calculate a last-step estimated extended key. (Pg. 21).

The Office Action admits that *Coppersmith* fails to recite "verifying the parameter A, to be right by detecting that the last-step estimated extended key can be calculated, calculating a right last-step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible."

However, *Ohkuma* also fails to teach or suggest "verifying the parameter A, to be right by detecting that the last-step estimated extended key can be calculated, calculating a right last-

step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible." *Ohkuma* teaches a maximum differential probability dp^f and maximum linear probability lp^f with respect to a function f(x) as an important measure for estimating the encryption strength of the function f(x). Thus, although *Ohkuma* teaches calculating the probability of a function, it does not teach calculating a function such that it is within a predetermined probability.

In the present invention, the probability of a false key surviving is the probability of the linear equation not to be impossible, and an expected value p that is the number of false keys to survive to $L + \mu$ of encryption equations is

$$p = 2^{\sigma} \times 2^{-\mu} \quad (9)$$

Therefore, $L + \mu$ of encryption equations satisfying $p << 1$ are prepared to allow the false keys to be eliminated. (Pg. 18).

Furthermore, one highly relevant inquiry in making an evaluation under 35 U.S.C. §103 is "[t]he relationship between the problem which the inventor. . . was attempting to solve and the problem to which any prior art reference is directed." *Stanley Works v. McKinney Mfg. Co.*, 216 USPQ, 298, 304 (Del. D.C. 1981). Thus, in analyzing the prior art under Section 103 of the Act, we must clearly comprehend the problem addressed by the present inventors and that problem must be compared or contrasted, as the case may be, with the problems addressed by the prior art. The present invention is directed towards estimating the cipher strength of a Feistel encryption algorithm while decrypting the algorithm. (Pg. 1). *Coppersmith*, however, is not directed towards determining the strength of the cipher. Likewise, *Ohkuma* is directed towards an encryption apparatus rather than an apparatus for determining the strength of the encryption.

Ohkuma is also directed towards an SPN type encryption system whereas the present invention is geared towards a Feistel encryption system.

Thus, both references are not directed towards the same subject matter of the present invention and do not recognize the same problem to be solved.

All arguments for patentability with respect to Claim 1 are repeated and incorporated herein for Claims 2-12.

If the Examiner believes a telephone interview will help further the prosecution of the case, the undersigned attorney can be contacted at the listed phone number.

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799